REMARKS

This communication is in response to the Office Action mailed June 29, 2005 in connection with the above-identified matter. Claims 1-13 were previously cancelled, without prejudice. Claims 14-26 remain pending in this application with claims 14 and 19 being the only independent claims. Reconsideration of the outstanding rejections in view of the amendments to the claims and remarks presented below is respectfully requested.

Claims 19-22 and 26 are rejected under 35 U.S.C. §103(a) as obvious over U.S. Patent No. 5,883,960 (the '960 patent) in view of U.S. Patent No. 5,799,086 (the '086 patent). Claims 23-25 are rejected under 35 U.S.C. §103(a) as obvious over the '960 patent and the '086 patent in view of U.S. Patent No. 5,557,679 (the '679 patent). Claims 14-16 are rejected under 35 U.S.C. §103(a) as obvious over the '960 patent and the '086 patent in view of U.S. Patent No. 6,188,899 (the '899 patent) and U.S. Patent No. 5,557,679 (the '679 patent). Claims 17 and 18 are rejected under 35 U.S.C. §103(a) as obvious over the '960, the '086, the '899, and the '679 patents in view of U.S. Patent No. 5,793,866 (the '866 patent).

Applicant respectfully traverses the Examiner's rejection of claims as described in detail below.

Independent Claim 19:

Addressing each limitation of claim 19 separately:

A. The Examiner maintains that the limitation from claim 19 of "A chip having a memory, wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored" is taught in Col. 7, line 40 through Col. 8, line 67 of the '960 patent. In the "Response to Arguments" section the Examiner states "Further '960 teaches that only the manufacturer of the mobile unit knows the KE_{MSNi}. Therefore it is inherent that the MSNi number is installed into the COB at time of manufacturer." (emphasis added) (Paragraph 4 of the June 29, 2005 Office Action)

Applicant expressly traverses this inherency argument and directs the Examiner's attention to the '960 patent that expressly teaches away from such interpretation.

The passage in question relied on by the Examiner reads:

> "FIG. 2 is a block diagram showing the configuration of the COB device 22 shown in FIG. 1. The COB device 22 comprises a CPU 30, a RAM 32, a

ROM 34, and an EEPROM 36; the whole structure is sealed with resin, and only a power supply terminal and an input/output terminal 38 for communication between the CPU 30 and the CPU 16 of the mobile unit are exposed. The structure is such that the contents of the internal EEPROM 36 cannot be read out or written in unless specific commands are input to the CPU 30 via the input/output terminal 38.

The ROM 34 contains a control program 40 for the CPU 30, a password 42, and a common public key KE_{COB} 44 corresponding to a common secret key KD_{COB} determined through consultation among all communication carriers concerned. The password 42 is stored to allow the user to enter the COB device 22 into a mode (supervisor mode) to carry out a specific command (to be described later) only when a value that matches the password 42 is entered via the input/output terminal 38.

...

KE_{COB} 44 is stored in order to enable a carrier public key KE_{Cj} (to be described later) which have been signature encrypted with KD_{COB} to be decrypted and then to be written into the EEPROM 36. That is, KE_{COB} B is stored so that only the person who knows KD_{COB} corresponding to KE_{COB} is authorized to write KE_{Cj}. These contents are written into the ROM 34 in the manufacturing process of the COB device 22 during the manufacture of the COB device before it is shipped to the mobile unit manufacturer. The contents are unalterable. The control program 40 includes programs for controlling input/output operations via the input/output terminal 38 as well as programs for encrypt/decrypt calculations expressed by equations (1) to (4), and all encrypt/decrypt operations in the mobile unit are performed within the COB device 22.

The EEPROM 36 can store personal information such as MSN, MSI, etc., a carrier public key KE_{Cj} 50 corresponding to a carrier secret key KD_{Cj} known only to the communications carrier, and a mobile unit public key KE_{MSNi} 52 corresponding to a mobile unit secret key KD_{MSNi} known only to the manufacturer of the mobile unit...

Of the contents of the EEPROM 36, the carrier public key KE_{Cj} 50 is written into the EEPROM 36 in the manufacturing process of the mobile unit. If one mobile unit model is approved by a plurality of communications carriers for connection, the same number of KE_{Cj}'s as the number of carriers are written. The mobile unit public key KE_{MSN}i 42 and ***the personal information 48 are written when the mobile unit is registered to the communications network.***" (emphasis added).

The limitation in question from claim 19 expressly calls for all three parameters (e.g., a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki) to be stored at the manufacturer of the chip. The passage quoted above provides that the public key KE_{COB} 44 may be written into ROM 34 in the manufacturing process of the COB device 22

before it is shipped to the mobile unit manufacturer. Applicant also acknowledges that the same passage discloses that personal identification such as MSN, MSI, etc., a carrier public key KE_{Cj} 50 corresponding to a carrier secret key KD_{Cj} known only to the communications carrier, and a mobile unit public key KE_{MSNi} 52 corresponding to a mobile unit secret key KD_{MSNi} known only to the manufacturer of the mobile unit may be stored in EEPROM 36. Unlike the carrier public key KE_{Cj} 50 that is written into the EEPROM 36 in the manufacturing process (Col. 8, ll. 48-50), the patent expressly states that the personal information (which expressly includes MSN as stated in Col. 8, ll. 36-37) is written "when the mobile unit is registered to the communications network" (Col. 8, ll. 54-55) rather during manufacture as called for in claim 19. In view of the fact that the '960 patent expressly teaches away from writing of any personal information, much less the claimed subscriber identification number (IMSI) and card number (ICCID), during the manufacturing process of the COB, applicant submits that claim 19 is patentable over the art of record.

B. Another limitation from claim 19 states "wherein the chip itself derives an initial secret key Ki_1 ***from the secret key Ki which is known and entered into the chip***" (emphasis added).

In rejecting claim 19, the Examiner acknowledges that the '960 patent fails to teach this limitation relying on the '086 patent as a secondary reference. Specifically, the passage of the '086 patent in question states,

> "Furthermore, the chip used in an embodiment of the present invention would have the ability to generate a public/private key pair for encryption and decryption of data and communications by the individual user. The cryptographic encryption keys may be of any acceptable asymmetric cryptographic types, such as RSA... The private key so generated is then stored inside the chips in a non-readable and tamper-resistant manner. In addition, the chip would also have the ability, once a public/private encryption key pair for that device has already been generated, to rekey and generate a new public/private encryption key pair in place of the previous key pair." (Col. 14, l. 66 through Col. 15, l. 17)

The limitation in question from claim 19 expressly calls for an initial secret key Ki_1 to be derived from the secret key Ki which is known and entered into the chip. The passage in question of the '086 patent quoted by the Examiner, at best, establishes that a chip may generate a public/private key pair. However, the reference fails to disclose or suggest that any secret key is derived from a secret key Ki which is known and entered into the chip, as found in claim 19.

C. The last limitation of claim 19 further specifies that "the chip in the terminal equipment is Toolkit-enabled and includes means for communicating with a security center (SC) and negotiating a new secret key Ki_2 for the chip".

It is the Examiner's position that this limitation is taught by the '960 patent at Col. 8, ll. 30-35 that reads "The control program 40 includes programs for controlling input/output operations via the input/output terminal 38 as well as programs for encrypt/decrypt calculations expressed by equations (1) to (4), and all encrypt/decrypt operations in the mobile unit are performed within the COB device 22."

This passage of the '960 patent fails to disclose or suggest that chip in the terminal equipment (i) is Toolkit-enabled; (ii) includes means for communicating with a security center (SC); and (iii) includes means for negotiating a new secret key Ki_2 for the chip. Instead, the '960 patent is silent as to whether the chip is Toolkit-enabled. In addition, the passage mentions programming for controlling input/output operations, but fails to disclose or suggest that such communication is with a security center. Lastly, the quoted text from the '960 patent mentions that the control program 40 includes programs for encrypt/decrypt calculations, however, it does not disclose whether such programming includes generating a new secret key Ki_2 for the chip, as expressly called for in claim 19. Accordingly, applicant submits that the Examiner has failed to establish a *prima facie* case of obvious providing a teaching for each and every element of the claim in question.

Dependent Claims 20, 21 and 26

As for dependent claims 20, 21 and 26, the Examiner maintains that the '960 patent reads on each element. However, the '960 patent is silent with respect to the claimed "security center" and the Examiner in rejecting these claims has failed to specify what element, if any, is analogous to the claimed "security center". Applicant submits that no security center is either disclosed or suggested by the '960 patent that performs all the functionality set forth in dependent claims 15, 20, 21, 24 and 26. For example, **claim 20** states "wherein the chip includes means for receiving data from the security center (SC)". The passage (Col. 3, ll. 49-63) cited by the Examiner in rejecting claim 20 merely establishes that the IC card includes means for receiving and transmitting information, but fails to expressly disclose or suggest that this communication is with a security center. **Claim 21** states "wherein the chip comprises a

microprocessor for negotiating a secret key with the security center (SC)". The text (Col. 7, l. 62 through Col. 8, l. 3) from the '960 patent cited by the Examiner teaches determining a secret key in accordance with a conventional cryptosystem, but fails to disclose or suggest that the secret key is negotiated with the security center, as claimed. **Claim 26** further specifies "wherein the chip includes means for reading data received from the security center (SC) in memory, modifying the data and transmitting the data to the security center (SC). The relevant passage (Col. 41, ll. 17-26 of the '086 patent) referred to by the Examiner in rejecting claim 26 merely discloses that the encryption pair key of the device may be rekeyed at any time after manufacture. The Examiner has failed to expressly state which element reads on the claimed "security center". Assuming, *arguendo*, that the "master escrow center" is analogous to the claimed "security center", in order for this passage to read on the claimed limitation it would have to teach that the chip reads data from the master escrow center, modifies that same data, and transmits the data modified data back to the master escrow center. Instead, the reference merely discloses that the master escrow center issues a new escrow certificate. Furthermore, applicant submits that the Examiner has failed to provide a motivation for modifying the '960 patent as taught by the '086 patent and therefore, has failed to establish a *prima facie* case of obviousness.

Independent Claim 14

Claim 14 has been rejected by the Examiner under 35 U.S.C. §103(a) as obvious over the '960 patent in view of the '086 patent, the '899 patent and the '679 patent. The preamble states, "wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored". This limitation is patentable over the prior art reference for the same reasons provide above with respect to independent claim 19 wherein the Examiner referred to the same passage of the prior art reference for teaching a similar claimed limitation as found in claim 19.

Limitation b) in the body of claim 14 states "the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip". The Examiner now refers to Col. 14, l. 66 through Col. 15, l. 17 of the '086 as a secondary reference that teaches this limitation. The relevant passage cited by the Examiner merely discloses that the chip itself may generate a private key or rekey for substitution of a previously generated key. However, the

reference fails to disclose or suggest that the chip itself derives a second secret key (initial secret Ki_1) from a secret key (Ki) which is known and entered into the chip. The claim expressly calls for a second secret key to be derived by the chip from a first secret key that is known and previously entered into the chip. In order to read on the claimed limitation the passage would have to state that rekeying is derived from a key previously stored in the chip. Furthermore, the Examiner has failed to provide a motivation as to why it would have been obvious to modify the '960 reference in view of the '086 patent.

The last passage of limitation b) states "while PIN and PUK are set to a default value". Again the Examiner acknowledges that this limitation is not taught by the '960, the '086 or the '899 reference and relies on yet a fourth reference, e.g., the '679 patent to teach this aspect of the claimed invention. Applicant submits that the Examiner has merely used the claim as a template. In combining references, the Examiner cannot "simply pick and choose among the elements of assorted" prior art disclosures; rather there must be some teaching or suggestion in the references to suggest the use in the particular claimed combination. *Smith Kline Diagnostics, Inc. v. Helena Labs. Corp.*, 958 F.2d 878, 8 USPQ2d 1468, 1475 (Fed. Cir. 1988). See also, *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988); *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303, 311 (Fed. Cir. 1983). Applicant submits that the Examiner in relying on four different references to reject the claimed invention in fact has succumbed to hindsight reconstruction using applicant's claimed invention as a template. As rationale for modifying the '960, '086 and '899 patents as taught by the'679 patent the Examiner states that the personal unblocking key adds to the safety but fails to establish any connection or relationship between the setting of default values for PIN and PUK with the personal unblocking key feature. Accordingly, applicant submits that absent improper use of the claimed invention as a template no reasonable motivation exits for modifying the references to render claim 14 obvious.

Furthermore, the passage (Col. 3, ll. 24-35 of the '679 patent) referred to by the Examiner states "Each retailer has data terminal equipment 9, to which are connected a reader 10 for SIM cards 11 and line encryption equipment 12, 13 consisting...For generating IMSI, Ki, and PUK". Unlike the '679 that discloses the generation of PIN and PUK values, instead claim 14 calls for the setting of these parameters to default values. Therefore, applicant submits that the rejection is improper in that it relies on hindsight reconstruction and, in the alternative, fails to read on

every element of the claimed invention and thus fails to set forth a *prima facie* case of obviousness.

Limitation c) calls for "making an entry in an authentication center (ACF) and a home location register (HLR) as soon as the subscriber has entered into a contract with a network operator". The Examiner acknowledges that neither the '960 nor the '086 patent teach this limitation relying instead on the '899 patent (Col. 6, l. 5 through Col. 7, l. 13) as a tertiary reference. The passage quoted by the Examiner is silent and makes no mention whatsoever of an authentication center or a home location register, much less, that such an entry in these devices occurs as soon as the subscriber has entered into a contract with a network operator.

Limitations d-f) state "d) "deriving at the authentication center (AC) the initial secret key Ki_1"; e) setting the conditions of the network so that during logon to the network a connection is established from the chip to the security center (SC) of the network operator; f) routing the connection from the chip to the security center (SC) during the first logon". The Examiner submits that these steps are taught in Col. 21, l. 19 through Col. 22, l. 7 of the '960 patent. Applicant maintains that the reference is silent as to an authentication center or security center and the Examiner has failed to expressly state which, if any, element of the '960 patent may be analogous to the claimed "authentication center" and "security center". As best understood, the passage fails to state where the secret key is derived, much less, that the key is derived at the authentication center, as claimed. If the Examiner is suggesting that the IC card registration terminal is analogous to the claimed "security center" then the patent fails to disclose or suggest that a connection is established from the chip to the security center, instead the IC card registration terminal sends the command to the internal COB. Lastly, the passage is silent as to when the command is sent from the IC card registration terminal to the internal COB, and thus fails to teach the routing of the connection from the chip to the security center during the first logon, as found in limitation f).

Limitation g) calls for the step of "negotiating between the chip and the security center (SC) a new second secret key Ki_2". Referring to the passage in question of the '086 patent (Col. 42, ll. 17-26) relied on by the Examiner in rejecting the claimed invention, once again it is unclear which element of the '086 patent the Examiner asserts is analogous to the claimed "security center". Presumably, the Examiner's position is that the "master escrow center" is analogous to the claimed "security center". However, the master escrow center's only stated

function is to transmit to the device the new escrow certificate not negotiate with the chip to generate a new secret key. The passage clearly does not disclose the generation of a new second secret key Ki_2 during negotiations between the chip and another device, much less, the security center.

Limitation h) further specifies the step of "unconditionally disabling the condition of step e)", wherein step e) provides for "setting the conditions of the network so that during logon to the network, a connection is established from the chip to the security center (SC) of the network operator". It is the Examiner's position that this limitation is taught by the '960 patent which states, "The control program 54, fixed patterns 56, mobile unit secret key KD_{MSNi}, and mobile unit public key KE_{MSNI} are written during the manufacture of the mobile unit, while the flag 58 is caused to change state when the mobile unit is registered to the communications network." (Col. 9, ll. 15-19) The '960 patent describes in Col. 9, ll. 2-3 the flag 58 as indicating "whether or not personal information has been written in the COB device 22". Accordingly, Col. 9, ll. 15-19 are to be interpreted to establish that when a mobile unit is registered to the communication network the state of flag 58 (i.e., a flag that has been previously set as a result of personal information having previously been written in the COB device 22) is to be changed or cleared. Applicant still maintains that the prior art of record is silent regarding disabling the setting of any conditions, much less, the setting of any conditions of the network so that during logon to the network, a connection is established from the chip to the security center (SC) of the network operator.

Dependent Claim 15

Claim 15 further calls for "the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established". In rejecting the claim the Examiner maintains this limitation is taught by Col. 8, ll. 21-29 of the '960 patent which reads,

> "KE_{COB} 44 is stored in order to enable a carrier public key KE_{Cj} (to be described later) which have been signature encrypted with KD_{COB} to be decrypted and then to be written into the EEPROM 36. That is, KE_{COB} is stored so that only the person who knows KD_{COB} corresponding to KE_{COB} is authorized to write KE_{Cj}. These contents are written into the ROM 34 in the manufacturing process of the

COB device 22 during the manufacture of the COB device before it is shipped to the mobile unit manufacturer."

This passage is entirely silent regarding an authentication center (AC), much less, transmitting and storing the initial secret key Ki_1 in the authentication center (AC) only after the contract is established. Instead, the text quoted above refers to storage of key information in the COB device 22.

Dependent Claims 17 and 18

Claim 17 states "wherein the home location register (HLR) is capable of setting and deleting a rerouting command (hotlining flag)". The Examiner acknowledges that this limitation is not disclosed in the '960, '086, '899 and '679 patents instead relying on a fifth reference, the '866 patent. Once again applicant submits that the Examiner has improperly used the claim as a template to piece different passages of numerous references together to render the present claimed invention obvious. Furthermore, the passage of the '866 patent cited by the Examiner states "The remote 104 performs verification functions....However, if the intruder changes the modulus, the derived value received from the central site will not bear the predetermined relationship to the intruder's modulus, and the device will flag the insertion of the intruder's modulus and abort the activation process." (emphasis added)(Col. 6, l. 45 – Col. 7, l. 4) This passage discloses abortion of the activation process, but is silent altogether concerning setting and deleting rerouting, as found in claim 17. In addition, claim 17 further specifies that it is the HLR which sets or deletes the rerouting command, which is not taught by the '866 patent.

Dependent Claim 18

Claim 18 states "wherein, when the initial secret key Ki_1 is entered into the authentication center (AC) for the first time, the hotlining flag is also set in the home location register (HLR)". The '866 patent, and in particular Col. 4, ll. 39-60 thereof cited by the Examiner, disclose an HLR and AC. However, the reference fails to disclose or suggest the entering of the initial secret key Ki_1 in the authentication center or the setting of the hotlining flag in the home location register. In addition, to these arguments, the Examiner has failed to

provide a motivation for modifying the '960, '086, '899 and '679 as taught by the '866 reference and thus has failed to establish a *prima facie* case of obviousness.

Dependent Claim 23

The Examiner acknowledges that the '096 and 086 patents fail to disclose or suggest "wherein PIN and PUK default values are stored at the chip", as found in claim 23. It is the Examiner's position that this limitation, is taught by the '679 patent in the passage (Col. 3, ll. 24-35) that reads "Each retailer has data terminal equipment 9, to which are connected a reader 10 for SIM cards 11 and line encryption equipment 12, consisting....For generating IMSI, Ki, and PUK". To the contrary, the '679 patent merely teaches that the central controller 1 contains means for generating IMSI, Ki and PUK, but still fails to disclose or suggest that these values are stored in the chip itself. Accordingly, applicant submits that since no reference discloses storing the default values of PIN and PUK at the chip itself, the Examiner has failed to establish a *prima facie* case of obviousness.

Dependent Claim 24

Claim 24 states "wherein step g) further comprises negotiating at the security center (SC) the PUK with the chip or generated in the security center (SC) and transmitted to the chip. The Examiner refers once again to Col. 3, ll. 24-35 of the '679 patent to teach this limitation. Applicant again traverses the Examiner's rejection and maintains that the passage merely discloses the generation of the PUK by the central controller 1, not negotiating at the security center the PUK with the chip nor generating the PUK in the security center and then transmitting it to the chip, as claimed.

Dependent Claim 25

Dependent claim 25 provides "wherein the PIN and PUK default values are stored at the chip". Again referring to the passage at Col. 3, ll. 24-35 of the '679 cited by the Examiner as the basis for the claim rejection and discussed above with respect to claim 24, the text only discloses the generation by the central controller 1 of the PIN and PUK values. The passage fails to expressly teach that such values are default values nor that these default values are stored at the chip itself, as found in claim 25.

For the foregoing reasons applicant submits that claims 14-26 are patentable over the prior art of record. Applicant submits that the application is in condition for allowance and passage to issuance is respectfully requested.

If any additional fees are required, authorization is hereby provided to charge our U.S. Patent and Trademark Deposit Account No. 14-1263.

Respectfully submitted,

Christa Hildebrand
Reg. No. 34,953
Attorney for Applicant(s)

Norris McLaughlin & Marcus P.A
875 Third Avenue, 18th Floor
New York, N.Y. 10017
Telephone: (212)808-0700
Facsimile: (212)808-0844